

Other threat group: Moses Staff

Names	Moses Staff (<i>self given</i>) Abraham's Ax (<i>self given</i>) DEV-0500 (<i>Microsoft</i>) Cobalt Sapling (<i>SecureWorks</i>) Marigold Sandstorm (<i>Microsoft</i>) Vengeful Kitten (<i>CrowdStrike</i>) White Dev 95 (<i>PWC</i>)
Country	 Iran
Motivation	Sabotage and destruction
First seen	2021
Description	(Check Point) In September 2021, the hacker group MosesStaff began targeting Israeli organizations, joining a wave of attacks which was started about a year ago by the Parisite, Fox Kitten, Pioneer Kitten and Agrius attack groups. Those actors operated mainly for political reasons in attempt to create noise in the media and damage the country's image, demanding money and conducting lengthy and public negotiations with the victims. MosesStaff behaves differently. The group openly states that their motivation in attacking Israeli companies is to cause damage by leaking the stolen sensitive data and encrypting the victim's networks, with no ransom demand. In the language of the attackers, their purpose is to "Fight against the resistance and expose the crimes of the Zionists in the occupied territories."
Observed	Sectors: Energy, Financial, Government, Manufacturing, Transportation, Utilities. Countries: Chile, Germany, India, Israel, Italy, Turkey, UAE, USA.
Tools used	DCSrv, PyDCrypt, StrifeWater.
Operations performed	Nov 2022 Abraham's Ax Likely Linked to Moses Staff < https://www.secureworks.com/blog/abrahams-ax-likely-linked-to-moses-staff >
Information	< https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/ > < https://www.cybereason.com/blog/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations > < https://www.fortinet.com/blog/threat-research/guard-your-drive-from-driveguard > < https://www.timesofisrael.com/report-iran-hacked-israeli-cameras-a-year-ago-defense-officials-knew-didnt-act/ >
MITRE ATT&CK	< https://attack.mitre.org/groups/G1009/ >

Card date: 10 March 2024

TLP: WHITE

This document has been created from the "Threat Group Cards: A Threat Actor Encyclopedia" portal, on a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License, by Digital Service Security Center
Electronic Transactions Development Agency

Report incidents

 +66 (0)2-123-1227

 helpdesk@etda.or.th

Follow us on

